Listing of Claims:

1. (Currently Amended) A method of accessing ~~access to~~ a service with fast authentication and revocable anonymity, ~~characterized in that it comprises~~ comprising the steps of:

i) identifying and registering a client [[(C)]] and providing the client [[him]] with means ~~for authenticating himself~~ configured to authenticate the client to an anonymous certification authority; [[(ACA),]]

ii) authenticating the client to the anonymous certification authority using the means provided in step i) and supplying the client with means configured to enable ~~enabling~~ the client [[him]] to authenticate the client ~~himself~~ anonymously to a server; [[(Se),]]

iii) authenticating the client by producing an anonymous signature and opening and maintaining an anonymous authentication session with the [[a]] server, wherein a unique anonymous signature is used for each session; [[(Se),]] and

iv) selectively allowing contact between the server [[(Se)]] and the anonymous certification authority [[(ACA)]] to revoke the anonymity of the client [[(C)]] using the anonymous signature provided in step iii[[)]].

2. (Currently Amended) The [[A]] method according to claim 1, further comprising: ~~characterized in that it comprises, before the step ii), an additional step of~~ communication between the anonymous certification authority [[(ACA)]] and the server, before the authenticating of the client to the anonymous certification authority, [[(Se)]] whereby the server [[(Se)]] presents to said anonymous certification authority [[(ACA)]] a request to obtain means enabling verification of the anonymous authentication supplied by a client [[(C)]].

3. (Currently Amended) The [[A]] method according to claim 1, ~~characterized in that~~ wherein the step iii [[)]] comprises ~~three stages~~:

a first stage in which the client [[(C)]] calculates data formed as ~~of~~ a series of tokens, wherein one of the series of tokens is configured to enable ~~of which one enables~~ a session to be opened and [[the]] others of the series of tokens are configured to enable ~~that~~ the session to be maintained; [[,]]

a second stage in which the client [[(C)]] makes a strong undertaking to the server as to the series of tokens; [[,]] and

a third stage of maintaining the session with the aid of the series of tokens.

4. (Currently Amended) The [[A]] method according to claim 3, ~~characterized in that~~ wherein [[all]] the series of tokens are configured for one-time use and each of the series of tokens are strongly interdependent.

5. (Currently Amended) The [[A]] method according to claim 3, ~~characterized in that~~ wherein the series of tokens are calculated using ~~the token generation step uses~~ two cryptographic primitives~~, namely a hashing function and a random number~~.

6. (Currently Amended) The [[A]] method according to claim 5, ~~characterized in that~~ wherein the first token W_i is obtained by applying a hashing function H to a random number, the second token W_z is obtained by applying the hashing function to the first token obtained, and so on until n tokens W_n are obtained:

$$H(W_0)=W_1 H(W_{n-1})=W_n.$$

7. (Currently Amended) The [[A]] method according to claim 3, ~~characterized in that~~ wherein the second stage comprises ~~includes~~ obtaining an anonymous signature of an initialization token [[W ~]] enabling authentication of the [[a]] client by the server.

8. (Currently Amended) The [[A]] method according to claim 7 [[3]], ~~characterized in that~~ wherein ~~information such as~~ a numerical value is associated with the initialization token.

9. (Currently Amended) The [[A]] method according to claim 3, ~~characterized in that~~ wherein on each new authentication the client [[(C)]] sends the server [[(Se)]] a token of at least one unit lower rank than that previously used.

10. (Currently Amended) The [[A]] method according to claim 3, ~~characterized in that~~ wherein on each new authentication the client [[(C)]] sends the server [[(Se)]] a token W_i whose rank (i) is ~~selected to be~~ representative of a ~~the~~ value of an operation~~, for example a number of bid increments~~.

11. (Currently Amended) The [[A]] method according to claim 3 [[1]], ~~characterized in that~~ wherein the steps are ~~it is~~ applied to bidding and [[the]] steps of the client [[(C)]] submitting an increased bid are effected by sending successive tokens of lower rank.

12. (Currently Amended) The [[A]] method according to claim 1, further comprising using ~~characterized in that it uses~~ a group signature by associating a plurality of identifiers and respective private keys with a single group public key.

13. (Currently Amended) The [[A]] method according to claim 1, ~~characterized in that~~ wherein the anonymous signature is ~~it uses~~ a blind signature.

14. (Currently Amended) The [[A]] method according to claim 12, ~~characterized in that~~ wherein a power ~~the powers~~ to revoke anonymity is shared ~~are divided~~ between two or more authorities.

15. (Currently Amended) A system adapted to open and maintain an authentication session guaranteeing non-repudiation, wherein an anonymous signature unique to the session and comprising a series of tokens is used to open and maintain each session, the system comprising: ~~characterized in that it comprises~~

means configured ~~adapted~~ to implement three stages:

a first stage in which [[the]] a client [[(C)]] calculates ~~data formed of a~~ the series of tokens, ~~of which~~ one of the series of tokens is configured to enable ~~enables~~ a session to be opened and another of the series of tokens is configured to enable the ~~others enable that~~ session to be maintained; [[,]]

a second stage in which the client [[(C)]] makes a strong undertaking to the server as to the series of tokens; [[,]] and

a third stage of maintaining the session with the aid of the series of tokens.

16. (Currently Amended) The system ~~A method~~ according to claim 15, ~~characterized in that~~ wherein the first stage calculates the series of tokens based on ~~token generation step uses~~ two cryptographic primitives, wherein the two cryptographic primitives are ~~namely~~ a hashing function and a random number.

17. (Currently Amended) The system ~~A method~~ according to claim 15, ~~characterized in that~~ wherein the system is configured to use ~~it uses~~ a group signature by associating a plurality of identifiers and respective private keys with a single group public key.

18. (Currently Amended) The system ~~A method~~ according to claim 15, ~~characterized in that it uses~~ wherein the unique anonymous signature is a blind signature.

19. (Currently Amended) The system ~~A method~~ according to claim 15, ~~characterized in that~~ wherein power ~~the powers~~ to revoke anonymity is [[are]] divided between two or more authorities.

20. (New) The method according to claim 5, wherein the two cryptographic primitives are a hashing function and a random number.

21. (New) The method according to claim 10, wherein the rank is representative of a number of bid increments.